IN THE CLAIMS

1.　　(currently amended)　A data processing apparatus for executing reproduction of data from a memory device or for recording of data into a memory device; ~~wherein~~

~~said data processing device has a structure for executing reproduction of data from said memory device or recording of data into said memory device~~ on condition that a mutual authentication between said data processing apparatus and said memory device is established; ~~and~~ comprising:

~~said data processing device further having:~~

a virtual memory device;

a structure ~~for~~ executing ~~a processing for~~ said mutual authentication with said ~~a~~ virtual memory device ~~set inside of said data processing apparatus in case~~ when said memory device ~~has~~ cannot function to execute ~~said processing for~~ said mutual authentication; and

a structure ~~for~~ executing said reproduction of data from said memory device or said recording of data into said memory device on condition that ~~said processing of the~~ mutual authentication ~~conducted~~ between said data processing apparatus and said virtual memory device is established.

2.　　(currently amended)　The data processing apparatus according to Claim 1~~,~~ ~~wherein~~

~~said data processing apparatus~~ further ~~includes~~ comprising a structure ~~for~~ executing ~~said processing of~~ the mutual authentication with ~~between~~ said memory device when said ~~processing of the~~ mutual authentication is available by initially checking whether said memory device ~~for executing data reproduction or data recording~~ is capable of executing said mutual authentication or not.

3.　　(currently amended)　The data processing apparatus according to Claim 1, further comprising: ~~including a structure wherein~~

~~such~~ a key for authenticating distribution of an enabling key block, ~~wherein~~ said ~~authenticating~~ key ~~is~~ having been previously enciphered by such ~~an~~ enabling key block containing ~~an~~ enciphering data for enciphering renewal keys on ~~such~~ paths ~~for~~ constituting a hierarchical key tree structure comprising a variety of keys disposed in correspondence with ~~such~~ tree roots, nodes, and leaves on ~~such~~ paths ranging from roots to leaves of said key tree

structure, the tree structure corresponding to comprising a plurality of data processing apparatuses as own leaves, wherein said enciphering data further comprisinges upper-rank keys in said tree hierarchy which are to be enciphered by lower-rank keys; and

said processing of the mutual authentication executed between said data processing apparatus and said virtual memory device is solely executed by applying said enabling key block distribution authenticating key and the other authenticating key previously stored in said virtual memory device.

4.   (currently amended)   The data processing apparatus according to Claim 3, wherein

only a properly licensed data processing apparatus is enabled to decode said enabling key block, whereas such a data processing apparatus devoid of a proper license is unable to decode said enabling key block in a plurality of data processing apparatuses jointly constituting leaves of said key tree structure; and

said data processing apparatus preventings such an improper data processing apparatus devoid of a proper license from illegally implementing mutual authentication with said virtual memory device by way of revoking said improper data processing apparatus.

5.   (currently amended)   The data processing apparatus according to Claim 3, further comprisingwherein

means for subjecting said enabling key block distribution authenticating key enciphered and presented by said enabling key block is subject to a version controlling process by way of executing a process for renewing individual versions.

6.   (currently amended)   The data processing apparatus according to Claim 1, further comprising:including a structure wherein

in a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, comprising a plurality of data processing apparatuses being associated with the tree as own leaves,

those means for enciphering leaf-keys provided in correspondence with own leaves are respectively enciphered by with a storage key proper to said individual ones of said

9

data processing apparatuses and then stor~~ing~~ed in a memory means inside of the corresponding data processing apparatus.

7.   (currently amended)   The data processing apparatus according to Claim 1, further comprising:~~including a structure wherein~~

~~in~~ a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on ~~such~~ paths ranging from roots to leaves of said key tree structure, there being ~~comprising~~ a plurality of data processing apparatuses corresponding to ~~as~~ own leaves, based on ~~those~~ leaf-keys provided in correspondence with own leaves,

a device key block stored in memory within the processing apparatus, the key block being ~~as~~ an assemblage of ciphered keys comprising mutually different individually enciphered node keys of plural steps ranging from own leaves up to upper-rank keys of said key tree structure ~~is stored in a memory means inside of said data processing apparatus~~.

8.   (currently amended)   A data processing method for executing reproduction of data from a memory device or for recording of data into said memory device, said data processing method comprising the steps of:

~~a step of~~ executing a mutual authentication process with a virtual memory device provided in said data processing apparatus ~~in the case in which~~ when said memory device is devoid of ~~such~~ a function to execute said mutual authentication; and

~~a step of~~ executing reproduction of data from said memory device or recording of data into said memory device ~~based on~~ conditioned on~~that~~ said mutual authentication ~~is~~ being actually effectuated between said data processing apparatus and said virtual memory device.

9.   (currently amended)   The data processing method according to Claim 8, further comprising the steps of:

~~a step of~~ identifying whether said memory device ~~for executing reproduction or recording of data~~ is capable of executing said mutual authentication ~~or not~~; and

~~a step of~~ executing a ~~processing for said~~ mutual authentication between said data processing apparatus and said memory device ~~in case~~ when ~~said~~ execution of said mutual authentication is possible.

10.   (currently amended)   The data processing method according to Claim 8,

wherein

said data processing apparatus comprises an enabling key block distribution authenticating key, wherein said authenticating key is previously enciphered by such an enabling key block containing data for enciphering renewal keys on such a path for constituting such which is part of a key tree structure withcomprising a variety of keys respectively disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, comprising a plurality of data processing apparatuses corresponding to as own leaves, wherein said enciphering key also includeing a data for enciphering upper-rank keys via lower-rank keys; wherein

said mutual authentication process executed between said data processing apparatus and said virtual memory device is solely being executed by applying said enabling key block distribution authenticating key and the other authenticating key previously stored in said virtual memory device.

11.   (currently amended) A license system for providing a data processing system with a proper license control, comprising:;

a means for providing an enabling key block distribution authenticating key previously enciphered by such an enabling key block containing data for enciphering renewal keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with root, nodes, and leaves on such a path ranging from roots to leaves of said key tree structure, comprising a plurality of data processing apparatuses as corresponding to own leaves, wherein said enabling key block also comprisinge such data for enciphering upper-rank keys via lower-rank keys;

a virtual memory device;

a means for executing a process for reproducing data from said memory device or recording data into said memory device solely based on conditioned on whether a that a mutual authentication is actually effectuated between said data processing apparatus and said memory device even when said memory device is devoid of a function to execute mutual authentication with said data processing apparatus; and

a means for enabling only such a properly licensed data processing apparatus to properly decode said enabling key block providing said enabling key block distribution

authenticating key among a plurality of data processing apparatuses for constituting said key tree structure and a~means for preventing such an improper data processing apparatus devoid of a proper license from illegally decoding said enabling key block, twhereby preventing said improper data processing apparatus from illegally effectuating authentication with said virtual memory device to further prevent said improper data processing apparatus from illegally utilizing contents data.

12.   (currently amended) A program providing medium which provides a computer system with a specific computer program for executing reproduction of data from a memory device or recording of data into a memory device; said computer program comprisinges:

a modulestep of executing a mutual authentication between a data processing apparatus and such a virtual memory device provided in a corresponding data processing apparatus in the case in which the above referred when the memory device is devoid of a function to execute mutual authentication; and

a module step of executing reproduction of data from said memory device or recording of data into said memory device solely based on conditioned uponthat said mutual authentication isbeing actually effectuated between said data processing apparatus and said virtual memory device.

13.   (previously presented) A data processing apparatus for recording data to, or reproducing data from, a memory device, the apparatus comprising:

a controller; and

a virtual memory;

wherein the recording of the data to, or reproduction of the data from, the memory device is conditioned upon the establishment of a mutual authentication between the controller and the virtual memory when the memory device does not support mutual authentication.

14.   (previously presented) The data processing apparatus of claim 13, wherein prior to performing the mutual authentication between the controller and the virtual memory, the controller checks if the memory device supports mutual authentication and, if so, the recording of the data to, or reproduction of the data from, the memory device is conditioned

upon the establishment of the mutual authentication between the controller and the memory device.

15.   (previously presented) The data processing apparatus of claim 13 wherein the mutual authentication is performed between the controller and the virtual memory by applying an authenticating key stored in the virtual memory and an enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the data processing apparatus is associated with one of the leaves of the key tree structure, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys.

16.   (previously presented) The data processing apparatus according to claim 15, wherein the data processing apparatus is properly licensed if the data processing apparatus is enabled to decode the enabling key block and wherein the data processing apparatus is devoid of proper licensing if unable to decode the enabling key block.

17.   (currently amended) The data processing apparatus according to claim 15 wherein the enabling key block distribution authenticating key enciphered by the enabling key block is subject to a version controlling process or by way of executing a process for renewing individual versions on the controller.

18.   (currently amended) The data processing apparatus according to claim 13 further comprising a memory for storing an enciphered leaf key, the enciphered leaf key produced by enciphering a leaf key with by a storage key that is associated with the data processing apparatus, and wherein the leaf key is being a part of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the leaf key is associated with the data processing apparatus.

19.   (previously presented) The data processing apparatus according to claim 13 further comprising a memory for storing a device key block comprising an assemblage of ciphered keys further comprising mutually different individually enciphered node keys of a

hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein one of the leaves is associated with the data processing apparatus.

20.   (previously presented) A method for use in a device for recording data to, or reproducing data from, a memory device, the method comprising the steps of:

(a)   executing a mutual authentication process with a virtual memory device when the memory device does not support the mutual authentication process; and

(b)   if the mutual authentication between the device and the virtual memory is successful, executing the recording of the data to, or the reproduction of the data from, the memory device.

21.   (previously presented) The method of claim 20 further comprising the steps of:

(c) prior to step (a), identifying whether the memory device supports the mutual authentication process; and

(d) if the memory device supports the mutual authentication process, skipping step (a) and executing the mutual authentication process with the memory device for the purpose of recording data to, or reproducing data from, the memory device.

22.   (previously presented)   The method of claim 20 wherein the mutual authentication process is executed between the device and the virtual memory by applying an authenticating key stored in the virtual memory and an enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the device is associated with one of the leaves of the key tree structure, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys.

23.   (currently amended) A license system for use in a data processing system, the license system comprising:

a—means for providing an enabling key block distribution authenticating key having been , wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein at least one of the leaves of the key tree structure is associated with a device, and wherein said enciphering data further comprisinges upper-rank keys to be enciphered by lower-rank keys;

a—means for executing a process for reproducing data from, or recording data to, a memory device solely based on conditioned on whether that a mutual authentication is actually effectuated between the device and the memory device even when the memory device is devoid of a function to execute mutual authentication with the device; and

wherein the device is being properly licensed if the device is enabled to decode the enabling key block and wherein the device beingis devoid of proper licensing if unable to decode the enabling key block.

24.   (currently amended) A computer-readable medium for storing computer-executable software code for the execution of the recording of data to, or the reproduction of data from, a memory device, said code comprising:

code for executing a mutual authentication process with a virtual memory device when the memory device does not support the mutual authentication process; and

code for executing the recording of the data to, or the reproduction of the data from, the memory device if the if the mutual authentication between the device and the virtual memory is successful.